

# Optimum Probe Parameters for Entangling Probe in Quantum Key Distribution

Howard E. Brandt

U.S. Army Research Laboratory

2800 Powder Mill Rd., Adelphi, MD 20783

## Abstract

For the four-state protocol of quantum key distribution, optimum sets of probe parameters are calculated for the most general unitary probe in which each individual transmitted photon is made to interact with the probe so that the signal and the probe are left in an entangled state, and projective measurement by the probe, made subsequent to projective measurement by the legitimate receiver, yields information

about the signal state. The probe optimization is based on maximizing the Renyi information gain by the probe on corrected data for a given error rate induced by the probe in the legitimate receiver. An arbitrary angle is included between the nonorthogonal linear polarization states of the signal photons. Two sets of optimum probe parameters are determined which both correspond to the same optimization. Also, a larger set of optimum probe parameters is found than was known previously for the standard BB84 protocol. A detailed comparison is made between the complete and incomplete optimizations, and the latter simpler optimization is also made complete. Also, the process of key distillation from the quantum transmission in quantum key distribution is reviewed, with the objective of calculating the secrecy capacity of the four-state protocol in the presence of the eavesdropping probe. Emphasis is placed on information leakage to the probe.

**Keywords:** quantum cryptography, quantum key distribution, quantum communication, quantum information processing

# 1 INTRODUCTION

Research efforts by many investigators have significantly advanced the field of quantum cryptography [1] since the pioneering discoveries of Wiesner [2] and Bennett and Brassard [3,4]. Emphasis has been placed on quantum key distribution, the generation by means of quantum mechanics of a secure random binary sequence which can be used together with the Vernam cipher (one-time pad) [5] for secure encryption and decryption. Various protocols have been devised for quantum key distribution, including the single-particle four-state Bennett-Brassard protocol (BB84) [3], the single-particle two-state Bennett protocol (B92) [6], and the two-particle entangled-state Einstein-Podolsky-Rosen (EPR) [7] protocol. However the original BB84 protocol is presently the most practical and robust protocol.

One effective implementation of the BB84 protocol [3] uses single photons linearly polarized along one of the four basis vectors of two sets of coplanar orthogonal bases oriented at an angle of 45 degrees (equivalently,  $\pi/4$ ) relative to each other. The polarization measurement operators in one basis do not commute with those in the other, since they correspond to nonorthogonal polarization states. At a fundamental level, the potential security of the

key rests on the fact that nonorthogonal photon polarization measurement operators do not commute, and this results in quantum uncertainty in the measurement of those states by an eavesdropping probe [8]. Before transmission of each photon, the transmitter and receiver each independently and randomly select one of the two bases. The transmitter sends a single photon with polarization chosen at random along one of the orthogonal basis vectors in the chosen basis. The receiver makes a polarization measurement in its chosen basis. Next, the transmitter and the receiver, using a public communication channel, openly compare their choices of basis, without disclosing the polarization states transmitted or received. Events in which the transmitter and the receiver choose different bases are ignored, while the remaining events ideally have completely correlated polarization states. The two orthogonal states in each of the two bases encode binary numbers 0 and 1, and thus a sequence of photons transmitted in this manner can establish a random binary sequence shared by both the transmitter and the receiver and can then serve as the secret key, following error correction and privacy amplification [9,10]. Privacy amplification is of course necessary, because of the possibility of an eavesdropping attack [1,3,4]. Using the Vernam cipher, the key can then be used to encode a message which can be securely trans-

mitted over an open communication line and then decoded, using the shared secret key at the receiver. (The encrypted message can be created at the transmitter by adding the key to the message and can be decrypted at the receiver by subtracting the shared secret key.)

Numerous analyses of various eavesdropping strategies have appeared in the literature. A recent review is given in [1]. The present work is limited to an individual attack in which each transmitted photon is measured by an independent probe after the photon polarization basis is revealed. In addition to the individual attack, other approaches include: coherent collective attacks in which the eavesdropper entangles a separate probe with each transmitted photon and measures all probes together as one system; and also coherent joint attacks in which a single probe is entangled with the entire set of carrier photons. However, these approaches require maintenance of coherent superpositions of large numbers of states, and this is not currently feasible

For the standard four-state (BB84) protocol [3] of key distribution in quantum cryptography, Slutsky, Rao, Sun, and Fainman [11] performed an eavesdropping probe optimization, which on average yields the most information to the eavesdropper for a given error rate caused by the probe. The

most general possible probe consistent with unitarity was considered [11–15], in which each individual transmitted bit is made to interact with the probe so that the carrier and the probe are left in an entangled state, and measurement by the probe, made subsequent to measurement by the legitimate receiver, yields information about the carrier state. The probe optimization is based on maximizing the Renyi information gain by the probe on corrected data for a given error rate induced by the probe in the legitimate receiver. A minimum overlap of the probe states which are correlated with the signal states (because of the entanglement) determines the maximum Renyi information gain by the probe. This is related to the idea that the more nearly orthogonal the correlated probe states are, the easier they are to distinguish. The upper bound on Renyi information gain by the probe is needed to calculate the secrecy capacity and to determine the number of bits which must be sacrificed during privacy amplification in order that it be exponentially unlikely that more than token leakage of the final key be available to the eavesdropper following key distillation. The results in [11] were obtained for the standard protocol with an angle of 45 degrees between the signal bases. The present work generalizes the probe optimization for arbitrary angle between the signal bases.

In Section 2, a detailed review is given of the optimization of the standard BB84 protocol by Slutsky et al [11]. In Section 3, the necessary conditions are obtained for the existence of possible extrema of the overlap of correlated probe states for an arbitrary angle between the signal bases. Section 4 identifies the possible extrema and associated probe parameters, and two sets of optimum probe parameters are determined which both correspond to the optimization. Section 5 determines an analytical algebraic expression for the maximum Renyi information gain by the probe for fixed error rate and angle between the signal bases. In Section 6, the simplified approach of Slutsky et al, which leads to the incomplete optimization, is made complete by recognizing certain necessary restrictions which were ignored by those authors. In Section 7, following a review of the process of key distillation, the secrecy capacity of the four-state protocol in the presence of the individual attack is calculated. Section 8 contains a summary. (The present work reviews the results of Refs. [12–14] by the author.)

## 2 PROBE OPTIMIZATION FOR STANDARD BB84 PROTOCOL

In this Section, the probe optimization of [11] is addressed for the standard BB84 protocol in which the angle between the signal bases is restricted precisely to  $\pi/4$  (equivalently,  $\alpha = \pi/8$  in Fig. 2 of [11]). From Section IV and Table II of [11], one has for the induced error rate  $E$  in the receiver by the eavesdropping probe,

$$E = \frac{P_{u\bar{u}} + P_{\bar{u}u}}{P_{u\bar{u}} + P_{\bar{u}u} + P_{uu} + P_{\bar{u}\bar{u}}}, \quad (1)$$

where  $P_{ij}$  is the probability that if a photon in polarization state  $|i\rangle$  is transmitted in the presence of the disturbing probe, the polarization state  $|j\rangle$  is detected by the legitimate receiver, where  $\{i, j\} = \{u, \bar{u}, v, \bar{v}\}$  corresponds to nonorthogonal polarization states  $|u\rangle$  and  $|v\rangle$ , and the state  $|\bar{u}\rangle$  orthogonal to  $|u\rangle$ , and  $|\bar{v}\rangle$  orthogonal to  $|v\rangle$ . The states  $|u\rangle$  and  $|v\rangle$  both correspond to Boolean state  $|1\rangle$ , and  $|\bar{u}\rangle$  and  $|\bar{v}\rangle$  correspond to Boolean state  $|0\rangle$ .

One has

$$P_{ij} = \langle \psi_{ij} | \psi_{ij} \rangle = |\psi_{ij}|^2, \quad (2)$$



where  $|\psi_{ij}\rangle$  is the projected state of the probe when polarization state  $|i\rangle$  is transmitted, and polarization state  $|j\rangle$  is detected by the receiver in the presence of the probe [11].

From Eqs. (1) and (8) of [11], it follows that

$$|\psi_{u\bar{u}}\rangle = \langle \bar{u} | U | u \otimes w \rangle, \quad (3)$$

where  $U$  is the unitary operator producing the entanglement of the probe state  $|w\rangle$  with the signal states, or

$$|\psi_{u\bar{u}}\rangle = (-\langle e_0 | \sin \alpha + \langle e_1 | \cos \alpha) U (|e_0\rangle \cos \alpha + |e_1\rangle \sin \alpha) \otimes |w\rangle, \quad (4)$$

where  $|e_0\rangle$  and  $|e_1\rangle$  are orthogonal basis vectors in the plane of the polarization states of the signal,  $|w\rangle$  is the initial state of the probe, and  $\alpha = \frac{1}{2}(\frac{\pi}{2} - \bar{\theta})$  is half the complement of the angle  $\bar{\theta} = \cos^{-1}(\langle u | v \rangle / |u||v|)$  between the two nonorthogonal linear-polarization states  $|u\rangle$  and  $|v\rangle$  of the signal (see Fig. 2 of [11]; I also refer to  $\bar{\theta}$  as the angle between the two orthogonal bases  $\{|u\rangle, |\bar{u}\rangle\}$  and  $\{|v\rangle, |\bar{v}\rangle\}$ .) Using Eq. (2) of [11] in Eq. (4), one obtains

$$|\psi_{u\bar{u}}\rangle = (-\langle e_0 | \sin \alpha + \langle e_1 | \cos \alpha) \left( \cos \alpha \sum_n |e_n\rangle \otimes |\Phi_{0n}\rangle + \sin \alpha \sum_n |e_n\rangle \otimes |\Phi_{1n}\rangle \right), \quad (5)$$

where  $|\Phi_{mn}\rangle$  are the unnormalized nonorthogonal states of the probe. Equa-

tion (5) becomes

$$|\psi_{u\bar{u}}\rangle = |\Phi_{01}\rangle \cos^2 \alpha - |\Phi_{10}\rangle \sin^2 \alpha + (|\Phi_{11}\rangle - |\Phi_{00}\rangle) \sin \alpha \cos \alpha, \quad (6)$$

and substituting Eq. (6) in Eq. (2), and using the symmetry properties of the probe states [11,15,16], and Eqs. (3a), (3b), and (12) of [11], one obtains

$$P_{u\bar{u}} = \frac{1}{2}(1 - d) + \frac{1}{2}(d - a) \sin^2 2\alpha - \frac{1}{2}c \sin 2\alpha. \quad (7)$$

where  $a, b, c,$  and  $d$ , expressed in terms of the eavesdropping probe parameters  $\lambda, \mu, \theta$ , and  $\phi$ , are given by [11,15,16]

$$a = \sin^2 \lambda \sin 2\mu + \cos^2 \lambda \cos 2\theta \sin 2\phi, \quad (8)$$

$$b = \sin^2 \lambda \sin 2\mu + \cos^2 \lambda \sin 2\phi, \quad (9)$$

$$c = \cos^2 \lambda \sin 2\theta \cos 2\phi, \quad (10)$$

$$d = \sin^2 \lambda + \cos^2 \lambda \cos 2\theta, \quad (11)$$

Summarizing Eq. (7), along with other results in Appendix C of [11], one has

$$P_{uu} = \frac{1}{2}(1 + d) - \frac{1}{2}(d - a) \sin^2 2\alpha + \frac{1}{2}c \sin 2\alpha, \quad (12)$$

$$P_{u\bar{u}} = \frac{1}{2}(1 - d) + \frac{1}{2}(d - a) \sin^2 2\alpha - \frac{1}{2}c \sin 2\alpha, \quad (13)$$

$$P_{\bar{u}u} = \frac{1}{2}(1 - d) + \frac{1}{2}(d - a) \sin^2 2\alpha + \frac{1}{2}c \sin 2\alpha, \quad (14)$$

$$P_{u\bar{u}} = \frac{1}{2}(1 + d) - \frac{1}{2}(d - a) \sin^2 2\alpha - \frac{1}{2}c \sin 2\alpha, \quad (15)$$

Substituting Eqs. (12)–(15) in Eq. (1), one obtains

$$E = \frac{1}{2} \left[ 1 - d + (d - a) \sin^2 2\alpha \right]. \quad (16)$$

Also from Section IV of [11], one has for the overlap  $Q$  of the probe states correlated with the signal received by the legitimate receiver:

$$Q = \frac{\langle \psi_{uu} | \psi_{\bar{u}\bar{u}} \rangle}{|\psi_{uu}| |\psi_{\bar{u}\bar{u}}|}, \quad (17)$$

or equivalently, using Eqs. (2) in Eq. (17), one obtains

$$Q = \frac{\langle \psi_{uu} | \psi_{\bar{u}\bar{u}} \rangle}{(P_{uu} P_{\bar{u}\bar{u}})^{1/2}}. \quad (18)$$

From Appendix C of [11], one also has

$$|\psi_{uu}\rangle = |\Phi_{00}\rangle \cos^2 \alpha + |\Phi_{11}\rangle \sin^2 \alpha + (|\Phi_{10}\rangle + |\Phi_{01}\rangle) \sin \alpha \cos \alpha, \quad (19)$$

and

$$|\psi_{\bar{u}\bar{u}}\rangle = |\Phi_{11}\rangle \cos^2 \alpha + |\Phi_{00}\rangle \sin^2 \alpha - (|\Phi_{10}\rangle + |\Phi_{01}\rangle) \sin \alpha \cos \alpha. \quad (20)$$

Using Eqs. (19), (20), the symmetry properties [11,15,16] of the probe states  $|\Phi_{ij}\rangle$ , and Eqs. (12), (3a), (3b) of [11], one obtains

$$\langle \psi_{uu} | \psi_{\bar{u}\bar{u}} \rangle = \frac{1}{2} (a + b) + \frac{1}{2} (d - a) \sin^2 2\alpha. \quad (21)$$

Next, substituting Eq. (21), (12) and (15) in Eq. (18), one obtains

$$Q = \left[ \frac{1}{2} (a + b) + (d - a) \frac{1}{2} \sin^2 2\alpha \right] \left[ \frac{1}{2} (1 + d) + (-d + a) \frac{1}{2} \sin^2 2\alpha + c \frac{1}{2} \sin 2\alpha \right]^{-\frac{1}{2}} \\ \times \left[ \frac{1}{2} (1 + d) + (-d + a) \frac{1}{2} \sin^2 2\alpha - c \frac{1}{2} \sin 2\alpha \right]^{-\frac{1}{2}}, \quad (22)$$

in agreement with Eq. (15) of [11]. The optimum information gain  $I_{opt}^R$  by the probe is given in terms of the overlap  $Q$  of correlated probe states by

$$I_{opt}^R = \log_2 (2 - Q^2) \quad (23)$$

(for the BB84 protocol, as well as the B92 protocol) [11,16–18]. It follows that  $I_{opt}^R$  is maximized when  $Q$  is minimized.

It is of interest to first limit the analysis to the standard BB84 protocol in which  $\alpha = \pi/8$ , corresponding to a 45-degree angle ( $\bar{\theta} = \pi/2 - 2\alpha = \pi/4$ ) between the signal bases and also between the two nonorthogonal polarization states  $|u\rangle$  and  $|v\rangle$  of the signal, namely,  $\langle u|v\rangle = \cos \bar{\theta} = \cos(\frac{\pi}{2} - 2\alpha) = \sin 2\alpha = \cos(\frac{\pi}{4}) = 2^{-1/2}$ . The conditional optimization in [11] is limited to this case. In that case, Eqs. (16) and (22) become

$$E_0 \equiv E_{|\alpha=\pi/8} = \frac{1}{2} \left[ 1 - \frac{1}{2} (d + a) \right], \quad (24)$$

and

$$Q_0 \equiv Q_{|\alpha=\pi/8} = \frac{\frac{1}{2}(d+a) + b}{\left\{ \left[ 1 + \frac{1}{2}(d+a) \right]^2 - \frac{1}{2}c^2 \right\}^{1/2}}, \quad (25)$$

respectively, in agreement with Eqs. (15) of [11]. Substituting Eq.(24) in Eq. (25), the latter becomes

$$Q_0 = \frac{1 - 2E_0 + b}{\left[ (2 - 2E_0)^2 - \frac{1}{2}c^2 \right]^{1/2}}, \quad (26)$$

also in agreement with Eq. (15) of [11].

For any value of  $E_0$ , the numerator of Eq. (26) has a conditional (fixed  $E_0$ ) minimum at some point where the denominator has a conditional maximum, namely,  $c = 0$ . (This is further substantiated in the following.) Clearly, the numerator of Eq. (26) for fixed  $E_0$  is minimum when  $b$  is minimum. Before minimizing  $b$ , substituting Eqs. (8) and (11) in Eq. (24), one obtains

$$E_0 = \frac{1}{2} - \frac{1}{4} \left[ \sin^2 \lambda (1 + \sin 2\mu) + \cos^2 \lambda \cos 2\theta (1 + \sin 2\phi) \right], \quad (27)$$

or

$$\sin 2\phi = \frac{2 - 4E_0 - \sin^2 \lambda (1 + \sin 2\mu)}{\cos^2 \lambda \cos 2\theta} - 1. \quad (28)$$

Next substituting Eq. (28) in Eq. (9), in order to eliminate the variable  $\phi$ , one gets

$$b = \sin^2 \lambda \sin 2\mu + \frac{2 - 4E_0 - \sin^2 \lambda (1 + \sin 2\mu)}{\cos 2\theta} - \cos^2 \lambda. \quad (29)$$

In order that  $b$  be minimum, so that  $Q_0$  can be minimum in Eq. (26), one requires that  $b$  in Eq. (29) satisfy

$$\frac{\partial b}{\partial \mu} = 0, \quad (30)$$

$$\frac{\partial b}{\partial \lambda} = 0, \quad (31)$$

and

$$\frac{\partial b}{\partial \theta} = 0. \quad (32)$$

Substituting Eq. (29) in Eqs. (30), (31), and (32), one requires

$$\sin^2 \lambda \cos 2\mu \left(1 - \frac{1}{\cos 2\theta}\right) = 0, \quad (33)$$

$$\sin 2\lambda (\sin 2\mu + 1) \left(1 - \frac{1}{\cos 2\theta}\right) = 0, \quad (34)$$

$$\frac{\sin 2\theta}{\cos^2 2\theta} [2 - 4E_0 - \sin^2 \lambda (1 + \sin 2\mu)] = 0. \quad (35)$$

Equations (33)–(35) are necessary conditions for minimum  $b$  and  $Q_0$ .

Equation (33) requires

$$(ia) \quad \sin \lambda = 0 \quad (36)$$

or

$$(ib) \quad \cos 2\mu = 0 \quad (37)$$

or

$$(ic) \quad \cos 2\theta = 1. \quad (38)$$

Equation (34) requires

$$(iia) \quad \sin 2\lambda = 0 \quad (39)$$

or

$$(iib) \quad \sin 2\mu = -1 \quad (40)$$

or

$$(iic) \quad \cos 2\theta = 1. \quad (41)$$

Equation (35) requires

$$(iiia) \quad \sin 2\theta = 0 \quad (42)$$

or

$$(iiib) \quad \sin^2 \lambda (1 + \sin 2\mu) = 2 - 4E_0. \quad (43)$$

A solution to Eqs. (33)–(35), which leads to the optimization given in [11], is given by

$$\sin \lambda = 0; \quad \sin 2\theta = 0; \quad \cos 2\theta = e_\theta \equiv \pm 1. \quad (44)$$

Equations (44) satisfy Eqs. (ia), (iia), and (iiia), and therefore also Eqs. (33)–(35). Next, substituting Eqs. (44) in Eq. (10), one gets

$$c = 0, \tag{45}$$

consistent with the conditional maximum of the denominator in Eq. (26), as declared above.

Furthermore, substituting Eqs. (44) in Eq. (28), one obtains

$$\sin 2\phi = \frac{2}{e_\theta} (1 - 2E_0) - 1. \tag{46}$$

Since only  $E_0 < 1/2$  is considered [11], and clearly  $E_0 \geq 0$ , then one requires

$$0 \leq E_0 < 1/2. \tag{47}$$

Then substituting Eq. (46) in Eq. (47), one requires

$$0 < e_\theta (\sin 2\phi + 1) \leq 2. \tag{48}$$

Clearly one requires  $e_\theta = +1$  because if  $e_\theta = -1$ , then Eq. (48) implies  $\sin 2\phi < -1$ , which is impossible. Therefore, one has in Eq. (44),

$$\cos 2\theta = e_\theta = 1, \tag{49}$$

and Eq. (48) becomes

$$-1 < \sin 2\phi \leq 1. \tag{50}$$



Next substituting Eqs. (44) and (49) in Eqs. (8)–(11), one requires

$$a = \sin 2\phi, \quad (51)$$

$$b = \sin 2\phi, \quad (52)$$

$$c = 0, \quad (53)$$

and

$$d = 1. \quad (54)$$

(Equation (53) restates Eq. (45).) Next substituting Eqs. (51) and (54) in Eq. (24), one obtains

$$E_0 = \frac{1}{4} (1 - \sin 2\phi), \quad (55)$$

and therefore

$$\sin 2\varphi = 1 - 4E_0. \quad (56)$$

Also, substituting Eqs. (52), (53) and (56) in Eq. (26), one obtains

$$Q_0 = 3 - \frac{2}{1 - E_0}. \quad (57)$$

Equations (57), (44), (49), and (50)–(55) agree with Eqs. (16) of [2]. The choice of  $\mu = 0$  in [11] is allowed because  $\mu$  only enters through  $a$  and  $b$  in Eqs. (8) and (9), and according to Eq. (44),  $\sin \lambda = 0$ . In general, however,

any  $\mu$  ( $0 \leq \mu \leq \pi$ ) produces the same optimization. Also,  $\lambda = \pi$  satisfies Eq.(44) as well as  $\lambda = 0$ . Other combinations of Eqs.(36)–(43) may also yield solutions, and this issue is addressed in Section 4 for arbitrary values of  $\alpha$ .

It is also well to further clarify the arguments of Appendix E in [11]. Note that according to Eq.(9) above,  $b$  is independent of  $\theta$ , and  $E_0$  in Eq.(27) is clearly least when  $\cos 2\theta = 1$ , since in the last term of Eq.(27),  $\cos^2 \lambda \geq 0$ , and according to Eq.(50),  $0 < (1 + \sin 2\phi) \leq 2$ . But then substituting Eq.(49) in Eq.(27), the latter becomes

$$E_0 = \frac{1}{2} - \frac{1}{4} \left[ 1 + \sin^2 \lambda \sin 2\mu + \cos^2 \lambda \sin 2\phi \right]. \quad (58)$$

Substituting Eq.(9) in Eq.(58), then

$$E_0 = \frac{1}{4} [1 - b], \quad (59)$$

which agrees with Eqs.(52) and (55). According to Eq.(59),  $E_0$  is a monotonically decreasing function of  $b$ , and the problem of minimizing  $b$ , subject to constant  $E$ , can be inverted so that  $E$  is minimized, subject to constant  $b$ . One also sees by substituting Eqs.(59) and (53) in Eq.(26) that Eq.(57) is again obtained, and since Eq.(57) results from minimizing  $b$  with

$E_0$  constant, this is equivalent to minimizing  $E_0$  with  $b$  constant, and is consistent with Appendix E of [11]. This approach to the optimization is further examined in section (6).

### 3 Extrema and Probe Parameters

In this Section, conditions for possible relative extrema are calculated of the overlap of correlated probe states of the Fuchs-Peres probe [11,15] for an arbitrary angle between the signal bases. Although the standard BB84 protocol with angle  $\pi/4$  between the signal bases will be seen to yield the most information to the probe, sensitivity to practical tuning variations in this angle can be useful in quantifying tolerances. First, Eq.(22) can be rewritten as

$$Q = \frac{\frac{1}{2}(a+b) + (d-a)\frac{1}{2}\sin^2 2\alpha}{\left\{\frac{1}{4}\left[1+d+(a-d)\sin^2 2\alpha\right]^2 - \frac{1}{4}c^2\sin^2 2\alpha\right\}^{1/2}}. \quad (60)$$

Also, from Eq. (16), it follows that

$$(d-a)\sin^2 2\alpha = 2E - 1 + d, \quad (61)$$

and substituting Eq. (61) in Eq. (60), one obtains

$$Q = \frac{\frac{1}{2}(a+b+d-1) + E}{\left\{(1-E)^2 - \frac{1}{4}c^2 \sin^2 2\alpha\right\}^{1/2}}. \quad (62)$$

From Eq. (61), it follows that

$$d = -\frac{2E - 1 + a \sin^2 2\alpha}{\cos^2 2\alpha}. \quad (63)$$

Next, using Eqs. (8), (9), and (63), and defining a quantity  $q$  to be  $[a+b+d]$ , one can show that

$$\begin{aligned} q \equiv a+b+d &= (2 - \tan^2 2\alpha) \sin^2 \lambda \sin 2\mu \\ &+ \cos^2 \lambda \sin 2\phi [1 + (1 - \tan^2 2\alpha) \cos 2\theta] - \frac{2E-1}{\cos^2 2\alpha}. \end{aligned} \quad (64)$$

Next substituting Eqs. (8) and (11) in Eq.(16), one has

$$\begin{aligned} E &= \frac{1}{2} \left[ 1 - \sin^2 \lambda - \cos^2 \lambda \cos 2\theta \right. \\ &\left. + \sin^2 2\alpha \left( \sin^2 \lambda + \cos^2 \lambda \cos 2\theta - \sin^2 \lambda \sin 2\mu - \cos^2 \lambda \cos 2\theta \sin 2\phi \right) \right]. \end{aligned} \quad (65)$$

It then follows from Eq. (65) that

$$\begin{aligned} \sin 2\mu &= \\ &\frac{\cos^2 \lambda (1 - \cos 2\theta) + \sin^2 2\alpha (\sin^2 \lambda + \cos^2 \lambda \cos 2\theta - \cos^2 \lambda \cos 2\theta \sin 2\phi) - 2E}{\sin^2 2\alpha \sin^2 \lambda}. \end{aligned} \quad (66)$$

Next substituting Eq. (66) in Eq. (64) to eliminate dependence on  $\mu$ , it follows

that

$$\begin{aligned}
q \equiv a + b + d = \cos^2 \lambda \{ (2 - \tan^2 2\alpha) [\cot^2 2\alpha - \cos 2\theta (\sin 2\phi + \cot^2 2\alpha)] \\
+ \sin 2\phi [1 + (1 - \tan^2 2\alpha) \cos 2\theta] \} - 4 \csc^2 2\alpha E + 3.
\end{aligned} \tag{67}$$

Also, substituting the definition of  $q$ , Eq. (64) in Eq. (62), one obtains

$$Q = \frac{\frac{1}{2}(q - 1) + E}{\left[ (1 - E)^2 - \frac{1}{4}c^2 \sin^2 2\alpha \right]^{1/2}}, \tag{68}$$

where  $q$  is given by Eq. (67),  $c$  is given by Eq. (10), and  $E$  is constant. Since  $q$  and  $c$  depend only on  $\lambda$ ,  $\theta$ , and  $\phi$ , and since  $E$  is constant, then  $Q$  depends only on the variables  $\lambda$ ,  $\theta$ , and  $\phi$ .

Possible extrema of the overlap  $Q$  for fixed  $E$  must satisfy

$$\frac{\partial Q}{\partial \lambda} = 0, \tag{69}$$

$$\frac{\partial Q}{\partial \theta} = 0, \tag{70}$$

$$\frac{\partial Q}{\partial \phi} = 0. \tag{71}$$

In general, Eqs. (69)–(71) may determine absolute or relative maximum, minimum, or saddle points in the space of probe parameters. The minimum  $Q$  is sought here. Possible solutions to Eqs. (69)–(71), giving the values of the probe parameters at the possible extrema, are derived in the Appendix. Each

possible solution corresponds to one of the combinations given by Eqs. (A-39)–(A-50), in which the fractions  $F_1, F_2$ , and  $F_3$  are defined by Eqs. (A-5), (A-10), and (A-15), respectively.

## 4 OPTIMUM PROBE PARAMETERS

Possible solutions to Eqs. (69)–(71) summarized in the Appendix by Eqs. (A-39)–(A-50) are designated by possibilities (A)–(L), respectively.

Possibilities (A), (C), (D) and (J) are excluded in the Appendix. Possibilities (B), (E)–(I), (K), and (L) all gave the same result, Eq. (A-60). However they differ in the values of the optimized probe parameters.

First consider possibility (B). According to Eqs. (A-51), (A-54), and (A-55), one has for the probe parameters  $\lambda$ ,  $\mu$ ,  $\theta$ , and  $\phi$ :

$$\sin \lambda = 0, \tag{72}$$

$$\cos 2\theta = 1, \tag{73}$$

$$\sin 2\phi = 1 - 2E \csc^2 2\alpha. \tag{74}$$

Evidently, according to Eqs. (72) and (66), the probe parameter  $\mu$  is arbitrary ( $0 \leq \mu \leq \pi$ ). In summary then for possibility (B), the optimized probe

parameters are:

$$\left\{ \lambda, \mu, \theta, \phi; \sin \lambda = 0, \cos 2\theta = 1, \sin 2\phi = 1 - 2E \csc^2 2\alpha \right\}. \quad (75)$$

Next consider possibility (E). According to Eqs. (A-134) and (A-135), one has

$$\cos \lambda = 0, \quad (76)$$

$$\sin 2\mu = 1 - 2E \csc^2 2\alpha. \quad (77)$$

Evidently  $\theta$  and  $\phi$  are arbitrary ( $0 \leq \theta \leq \pi, 0 \leq \phi \leq \pi$ ). Thus for possibility (E), the optimized probe parameters are

$$\left\{ \lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 2E \csc^2 2\alpha \right\}. \quad (78)$$

For possibility (F), according to Eqs. (A-141), (A-146), (A-143), and (A-147), the optimized probe parameters are:

$$\left\{ \lambda, \mu, \theta, \phi; \sin 2\mu \sin^2 \lambda = 1 - 2E \csc^2 2\alpha \mp \cos^2 \lambda, \cos 2\theta = 1, \sin 2\phi = \pm 1 \right\}. \quad (79)$$

For possibility (G), according to Eqs. (A-148), (A-150), (A-152), and (A-154), the optimized probe parameters are:

$$\left\{ \lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 2E \csc^2 2\alpha, \cos 2\theta = 1 \right\}, \quad (80)$$

or

$$\left\{ \lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 2E \csc^2 2\alpha, \sin 2\phi = 1 - 2 \cot^2 2\alpha, \cos 2\theta = e_\theta \right\}, \quad (81)$$

Equations (80) and (81) are apparently included in Eq. (78).

For possibility (H), according to Eqs. (A-160) and (A-162), one has

$$\left\{ \lambda, \mu, \theta, \phi; \sin 2\mu \sin^2 \lambda = 1 - 2E \csc^2 2\alpha - \cos^2 \lambda \sin 2\phi, \cos 2\theta = 1 \right\}. \quad (82)$$

Evidently Eqs. (75) and (79) are included in Eq. (82).

For possibility (I), according to Eqs. (A-163), (A-165), (A-167), and (A-168), one has

$$\left\{ \lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 2E \csc^2 2\alpha, \cos 2\theta = 1 \right\}, \quad (83)$$

or, alternatively,

$$\left\{ \lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 2E \csc^2 2\alpha, \sin 2\phi = 1 - 2 \cot^2 2\alpha \right\}. \quad (84)$$

Equations (83) and (84) are evidently included in Eq. (78).

For possibility (K), according to Eqs. (A-174), (A-177), and (A-179), the



optimum probe parameters are:

$$\left\{ \lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 2E \csc^2 2\alpha, \sin 2\phi = 1 - 2 \cot^2 2\alpha \right\}. \quad (85)$$

Comparing Eq. (85) with Eq. (78), it is evident that Eq. (85) is included in Eq. (78)

Finally, for possibility (L), according to Eqs. (A-186), (A-188) and (A-189), the optimum probe parameters are

$$\left\{ \lambda, \mu, \theta, \phi; \sin 2\mu \sin^2 \lambda = 1 - 2E \csc^2 2\alpha - \cos^2 \lambda \sin 2\phi, \cos 2\theta = 1, \right. \\ \left. \cos^2 \lambda = 2(1 - E)^2 (1 - 2 \cot^2 2\alpha - \sin 2\phi) \right. \\ \left. \times \left[ \sin^2 2\alpha \cos^2 2\phi [1 + (1 - 2 \csc^2 2\alpha) E] \right]^{-1} \right\}. \quad (86)$$

Comparing Eqs. (86) with Eq. (78), one sees that Eq. (86) is included in Eq. (82).

Equations (78) and (82) are different possible sets of optimized probe parameters, both of which correspond to the same optimization, Eq. (A-60).

In summary, the optimized sets of probe parameters are:

$$\left\{ \lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 2E \csc^2 2\alpha \right\}, \quad (87)$$

$$\left\{ \lambda, \mu, \theta, \phi; \sin 2\mu \sin^2 \lambda = 1 - 2E \csc^2 2\alpha - \cos^2 \lambda \sin 2\phi, \cos 2\theta = 1 \right\}. \quad (88)$$

For  $\alpha = \pi/8$ , these reduce to

$$\{\lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 4E\}, \quad (89)$$

$$\{\lambda, \mu, \theta, \phi; \sin 2\mu \sin^2 \lambda = 1 - 4E - \cos^2 \lambda \sin 2\phi, \cos 2\theta = 1\}. \quad (90)$$

Equation (90), for  $\sin \lambda = 0$ , corresponds to the standard optimization in [2] and in Section 2 above, but, other than that, the two sets of optimized probe parameters given by Eqs. (89) and (90) were not found by the simplified arguments appearing there. (Still another set of solutions, holding only for  $\alpha = \pi/4$ , follows from Eq. (A-173), and is addressed in Section 6.) Both Eqs. (89) and (90) (together with Eqs. (8)–(11), (24), and (26)) yield Eq. (57). It can also be shown that all sets of optimum probe parameters following from Eqs. (36)–(43) are subsets of Eq. (88), and also yield Eq. (57).

## 5 MAXIMUM INFORMATION GAIN

In Section 4 and the Appendix, it was determined that the only remaining possible extremum of the overlap  $Q$  of correlated probe states for fixed error rate  $E$  is given by Eq. (A-60), namely,

$$Q = \frac{1 + (1 - 2 \csc^2 2\alpha)E}{1 - E}. \quad (91)$$

I have found that if one plots points using the general expression for the nonoptimized overlap given by the parametric Eqs. (60) and (16) along with Eqs. (8)–(11) for a representative range of values of the error rate  $E$  and the probe parameters  $\lambda$ ,  $\mu$ ,  $\theta$ , and  $\phi$ , for a range of  $\alpha \leq \pi/8$ , the nonoptimized values of  $Q$  all lie above the corresponding curves given by Eq. (91). Also, by explicitly calculating the difference between the optimized overlap, Eq. (91), and the nonoptimized overlap, Eqs. (60) and (16), for representative ranges of the error rate and the probe parameters in the neighborhood surrounding each of the optimized sets, Eqs. (87) and (88), I have found that for  $\alpha = \pi/8$  or  $\pi/9$ , the nonoptimized overlap is not decreasing, and therefore Eq. (91) does in fact represent a minimum. Also, it is evident from Eq. (91) that the minimum overlap  $Q$ , for constant  $E$ , decreases as  $\alpha$  decreases below  $\pi/8$ . Apparently, the optimization holds for  $\alpha \leq \pi/8$ . However, for  $\alpha > \pi/8$ , this is not the case (points resulting from Eqs. (60) and (16) fall above and below the curves given by Eq. (91)), and therefore the extremization does not correspond to a minimum for  $\alpha > \pi/8$ . (For example, if  $\alpha = \pi/8 + 10^{-6}$ ,  $E = 0.2$ ,  $\mu/\pi = 0.156816$ ,  $\lambda/\pi = 0.3$ ,  $\theta/\pi = 0.1$ , and  $\phi/\pi = 0.75$ , one obtains, using Eqs. (16), (60), and (8)–(11), the value  $Q = 0.500003$  for the nonoptimized overlap; but Eq. (91) yields a larger value,  $Q = 0.500004$ . Also,

if  $\alpha = \pi/5$ ,  $E = 0.3$ ,  $\mu/\pi = 0.0711275$ ,  $\lambda/\pi = 0.7$ ,  $\theta/\pi = 0.7$ , and  $\phi/\pi = 0.7$ , one obtains  $Q = 0.34828$  for the nonoptimized overlap, but Eq. (91) yields  $Q = 0.909509$ .)

However, it is at this point essential to note the invariance of the Error rate  $E$ , Eq. (1), and the overlap  $Q$ , Eq. (17), under an interchange of the states  $|u\rangle$  and  $|\bar{u}\rangle$ ; thus

$$\{E, Q\} \xrightarrow{|u\rangle \leftrightarrow |\bar{u}\rangle} \{E, Q\}. \quad (92)$$

Also, from Fig. 2 of [11], it is evident that under the interchange of  $|u\rangle$  and  $|\bar{u}\rangle$ , the angle  $\bar{\theta}$  between the nonorthogonal polarization states becomes  $2\alpha$ ; thus

$$\bar{\theta} \xrightarrow{|u\rangle \leftrightarrow |\bar{u}\rangle} 2\alpha, \quad (93)$$

or equivalently, since  $\bar{\theta} = \frac{\pi}{2} - 2\alpha$ ,

$$\alpha \xrightarrow{|u\rangle \leftrightarrow |\bar{u}\rangle} \frac{\pi}{4} - \alpha. \quad (94)$$

Also, using Eq. (94), one has

$$\{\alpha \leq \pi/8\} \xrightarrow{|u\rangle \leftrightarrow |\bar{u}\rangle} \{\alpha \geq \pi/8\}. \quad (95)$$

It then follows from Eqs. (91), (94), and (95) that the optimum overlap,

$$Q = \frac{1 + (1 - 2 \csc^2 2\alpha) E}{1 - E}, \quad \alpha \leq \pi/8, \quad (96)$$

becomes

$$Q = \frac{1 + \left(1 - 2 \csc^2 2 \left(\frac{\pi}{4} - \alpha\right)\right) E}{1 - E}, \quad \alpha \geq \pi/8, \quad (97)$$

or equivalently,

$$Q = \frac{1 + (1 - 2 \sec^2 2\alpha) E}{1 - E}, \quad \alpha \geq \pi/8. \quad (98)$$

Also, the optimized sets of probe parameters, Eqs. (87) and (88), namely,

$$\left\{ \lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 2E \csc^2 2\alpha \right\}, \quad \alpha \leq \pi/8, \quad (99)$$

$$\left\{ \lambda, \mu, \theta, \phi; \sin 2\mu \sin^2 \lambda = 1 - 2E \csc^2 2\alpha - \cos^2 \lambda \sin 2\phi, \cos 2\theta = 1 \right\}, \quad \alpha \leq \pi/8, \quad (100)$$

become, for  $\alpha \rightarrow \frac{\pi}{4} - \alpha$  :

$$\left\{ \lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 2E \sec^2 2\alpha \right\}, \quad \alpha \geq \pi/8, \quad (101)$$

$$\left\{ \lambda, \mu, \theta, \phi; \sin 2\mu \sin^2 \lambda = 1 - 2E \sec^2 2\alpha - \cos^2 \lambda \sin 2\phi, \cos 2\theta = 1 \right\}, \quad \alpha \geq \pi/8. \quad (102)$$

I have found that if one plots points using the general expression for the nonoptimized overlap, given by the parametric Eqs. (60) and (16) along with Eqs. (8)–(11), for a representative range of values of the error rate  $E$  and the probe parameters  $\lambda$ ,  $\mu$ ,  $\theta$ , and  $\phi$ , for a range of  $\alpha \geq \pi/8$ , the nonopti-

mized values of  $Q$  all lie above the corresponding curves given by Eq. (98).

Apparently, for  $\alpha \geq \pi/8$ , the optimization, Eq. (98), holds.

With the restrictions on  $\alpha$ , the maximum Renyi information gain by the probe is given by Eq. (23), namely, [11–14]

$$I_{opt}^R = \log_2(2 - Q^2), \quad (103)$$

where  $Q$  is given by Eq. (96) for  $\alpha \leq \pi/8$ , and Eq.(98) for  $\alpha \geq \pi/8$ , or

$$Q = \begin{cases} \frac{1+(1-2\csc^2 2\alpha)E}{1-E}, & \alpha \leq \pi/8 \\ \frac{1+(1-2\sec^2 2\alpha)E}{1-E}, & \alpha \geq \pi/8 \end{cases}. \quad (104)$$

Thus for the BB84 protocol, one has

$$I_{opt}^R = \begin{cases} \log_2 \left( 2 - \left[ \frac{1+(1-2\csc^2 2\alpha)E}{1-E} \right]^2 \right), & \alpha \leq \pi/8 \\ \log_2 \left( 2 - \left[ \frac{1+(1-2\sec^2 2\alpha)E}{1-E} \right]^2 \right), & \alpha \geq \pi/8 \end{cases}. \quad (105)$$

For  $\alpha = \pi/8$ , Eq. (105) produces Fig. 6 of [11], as it must. Also,  $I_{opt}^R$  in Eq. (105) increases as  $\alpha$  decreases below  $\pi/8$ , or increases above  $\pi/8$ . As is to be expected, it is also evident from Eq. (105). that the standard BB84 protocol with  $\alpha = \pi/8$  yields less information than for any other value of  $\alpha$ .

## 6 OPTIMIZATION COMPARISON

As reviewed above in Section 2, Slutsky, et al [11] had earlier argued that for the standard BB84 protocol (with  $\alpha = \pi/8$ ), the optimum set of probe parameters is given by (See Eqs. (16) of Ref. [11].):

$$\{\lambda, \mu, \theta, \phi; \lambda = 0, \mu = 0, \cos 2\theta = 1, \sin 2\phi = 1 - 4E\}. \quad (106)$$

In obtaining Eq. (106), Slutsky et al made certain simplifying assumptions, based on the algebraic form of the overlap function, which yielded the correct maximum Renyi information gain, but an incomplete set of optimum probe parameters. In this section, a detailed comparison is made between the optimization of Ref. [11] and the complete optimization of Section 5.

A solution to Eqs. (33)–(35), and (28) is

$$\{\lambda, \mu, \theta, \phi; \sin \lambda = 0, \cos 2\theta = 1, \sin 2\phi = 1 - 4E\}. \quad (107)$$

Note that Eqs. (107) and (10) give  $c = 0$ , consistent with the above. Since  $\mu$  enters Eqs. (26) and (24) only through the term  $\sin^2 \lambda \sin 2\mu$  in Eqs. (8) and (9), and since  $\sin 2\mu \sin^2 \lambda = 0$ , the choice  $\sin 2\mu = 0$  yields a possible solution, which when combined with Eq. (107) gives the set

$$\{\lambda, \mu, \theta, \phi; \sin 2\mu = 0, \sin \lambda = 0, \cos 2\theta = 1, \sin 2\phi = 1 - 4E\}, \quad (108)$$

consistent with Eq. (106) and a subset of Eq. (90).

It is to be noted that a more general solution to Eqs. (33)–(35) is given by

$$\{\lambda, \mu, \theta; \cos 2\theta = 1\}, \quad (109)$$

which when combined with Eq. (28) yields

$$\{\lambda, \mu, \theta, \phi; \cos 2\theta = 1, \sin 2\mu \sin^2 \lambda = 1 - 4E - \cos^2 \lambda \sin 2\phi\}, \quad (110)$$

coinciding with Eq. (90). One therefore sees that even with the assumptions of Ref. [11], a more general set than Eq. (106) obtains, namely, Eq. (110). Furthermore, to obtain a more complete optimization, one must consider the case

$$\cos \lambda = 0, \quad (111)$$

in which case Eq. (28) is not defined. Instead, using Eqs. (8), (11) and (24), one obtains

$$\sin^2 \lambda \sin 2\mu = 1 - 4E + \cos^2 \lambda [1 - \cos 2\theta (1 + \sin 2\phi)], \quad (112)$$

and substituting Eq. (112) in Eq. (9), one gets

$$b = 2 - 4E - \cos^2 \lambda \cos 2\theta (1 + \sin 2\phi) - \sin^2 \lambda + \cos^2 \lambda \sin 2\phi. \quad (113)$$



For minimum  $b$ , one then requires

$$\frac{\partial b}{\partial \phi} = 0, \quad \frac{\partial b}{\partial \lambda} = 0, \quad \frac{\partial b}{\partial \theta} = 0. \quad (114)$$

Therefore substituting Eq. (113) in Eqs. (114), one obtains

$$\cos^2 \lambda (1 - \cos 2\theta) \cos 2\phi = 0, \quad (115)$$

$$\sin \lambda \cos \lambda (1 + \sin 2\phi) (1 - \cos 2\theta) = 0, \quad (116)$$

$$\cos^2 \lambda (1 + \sin 2\phi) \sin 2\theta = 0. \quad (117)$$

One observes that Eqs. (115)–(117) are in fact satisfied by Eq. (111), and from Eqs. (111) and (112), one obtains the optimization, Eq. (89),

$$\{\lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 4E\}, \quad (118)$$

which is the missing set in the optimization of Ref. [11].

It is evident that Eqs. (115)–(117) are also satisfied by  $\sin 2\phi = -1$ , and combining this with Eq. (112), one obtains an additional set of optimum probe parameters:

$$\{\lambda, \mu, \theta, \phi; \sin 2\phi = -1, \sin 2\mu \sin^2 \lambda = 1 - 4E + \cos^2 \lambda\}. \quad (119)$$

This solution was also not obtained in Ref. [11]. It is at this point important to note that, since the analysis in Sections 3 and 4 and Ref. [12] was

performed for arbitrary  $\alpha$ , the possible solution given by Eq. (A-48) was ignored because it followed from Eq. (A-173) that  $\alpha = \pi/8$  and  $e_\phi = -1$  are required. However, if  $\alpha = \pi/8$ , then Eqs. (A-48) and (57) are satisfied for the set of probe parameters given by Eq. (119).

Also, Appendix E of Ref. [11] addresses an alternative simplification of the optimization problem, which is reviewed in the above at the end of Section 2. The problem is inverted so that  $E$  is minimized subject to constant  $b$ , arguing that the conditional minimum of  $E$  is a monotonically decreasing function of  $b$  for the domain of interest ( $0 \leq E < 1/2$ ). In Eq. (59)  $E$  is seen to be a monotonically decreasing function of  $b$ , as claimed in Appendix E of Ref. [11]. Furthermore, since in this case  $\cos 2\theta = 1$ , then, together with Eq. (112), one obtains the set of optimum probe parameters,

$$\left\{ \lambda, \mu, \theta, \phi; \cos 2\theta = 1, \sin 2\mu \sin^2 \lambda = 1 - 4E - \cos^2 \lambda \sin 2\phi \right\}, \quad (120)$$

in agreement with Eq. (90). However, the optimization given in Ref. [11], namely Eq. (106) above, is a subset of Eq. (120). Furthermore, if the multiplier  $\cos \lambda$  of  $\cos 2\theta$  in Eq. (27) is vanishing, then  $\cos 2\theta = 1$  does not necessarily produce the best  $E_0$ . Thus if

$$\cos \lambda = 0, \quad (121)$$

then combining this with Eq. (27) yields the optimum set,

$$\{\lambda, \mu, \theta, \phi; \cos \lambda = 0, \sin 2\mu = 1 - 4E\}, \quad (122)$$

which is again the missing set, Eq. (89).

Also, if  $\sin 2\phi = -1$ , then the multiplier of  $\cos 2\theta$  in Eq. (27) is again vanishing, and then  $\cos 2\theta = 1$  does not necessarily produce the best  $E_0$ , but  $\sin 2\phi = -1$  along with Eq. (27) again leads to the optimization given by Eq. (119). It can also be shown that  $\cos 2\theta = 0$ , for which Eq. (28) is also not satisfied, leads to no additional optimum sets of probe parameters.

## 7 SECRECY CAPACITY

The maximum Renyi information gain, Eq. (105), can be used to calculate the secrecy capacity of the four-state protocol in the presence of the individual attack. Before calculating the secrecy capacity, a review of key distillation is at this point appropriate. Let  $m$  bits of raw data be received by the legitimate receiver in the four-state quantum-key-distribution protocol, and suppose  $n$  bits of sifted data remain following removal of  $(m - n)$  inconclusive bits, and suppose there are  $e_T$  bits of erroneous data, leaving  $(n - e_T)$  bits of corrected data. Corrected data includes data remaining af-

ter discarding inconclusive results and also erroneous data as determined by block checksums and bisection search. Privacy amplification is the procedure for obtaining a more secure, but shorter, key. This is achieved by removing from the  $(n - e_T)$  bits of corrected data a number  $s$  of bits (the privacy amplification compression level) that is the sum of the possible contributions to information leakage. There then remain  $(n - e_T - s)$  bits, and this is the size of the final key. The privacy amplification compression level  $s$  is given by [19]

$$s = t(n, e_T) + q + \nu + g, \quad (123)$$

where  $q$  is the estimated information leakage during error correction,  $\nu$  is the estimated leakage from any multi-photon bits,  $g$  is an extra safety margin, and  $t(n, e_T)$  is the defense function. The defense function, in general, depends on the size  $n$  of the sifted data, and on the number  $e_T$  of errors, and is chosen appropriately by the legitimate users, in order to effectively defend against an eavesdropping attack. The defense function  $t(n, e_T)$  is the estimated upper bound on possible information leakage through eavesdropping on the quantum channel. Quantitatively it is determined by the maximum total Renyi information gain  $I_T^R$  by the eavesdropping probe. (It is proved in [11] that

the optimum individual attack maximizes both the Renyi and Shannon information gain by the eavesdropping probe.) The maximum Renyi information gain by the eavesdropper is based on minimizing the overlap of the measured probe states correlated with the disturbed signal states of the legitimate receiver, conditional on fixed induced error rate. The compression level  $s$  must be chosen so that the probability is small that  $I_T^R > t(n, e_T)$ . An attack is successful if it introduces  $e_T$  errors on the  $n$  bits of sifted data, and yields a Renyi information  $I_T^R > t(n, e_T)$  on the  $(n - e_T)$  bits of corrected data. The probability of a successful attack must be negligible. In the presence of noise and channel losses, it is not sufficient, for the security of a quantum key distribution system, to detect eavesdropping. It must be insured that the shared data is sufficiently secure.

It is well to recall the privacy amplification theorem [9]. First, however, recall the definition of the Renyi information  $I^R(l)$  on an  $l$  bit string  $X$  having probability distribution  $P_X(X)$ , namely,

$$I^R(l) = l + \log_2 \langle P_X(X) \rangle = l + \log_2 \sum_X P_X^2(X), \quad (124)$$

where the bracket denotes the expectation value. ( $P_X^2(X)$  is often referred to as the collision probability.) The privacy amplification theorem states that

if the eavesdropper's Renyi information gain  $I^R(l)$  on an  $l$  bit data string is less than some quantity  $r$ , namely,

$$I^R(l) \leq r, \quad (125)$$

then the eavesdropper's Shannon information  $I^H(l-s)$  on the reduced  $(l-s)$  bit string, averaged over the choice of privacy amplification hash function, is bounded above, namely,

$$\langle I^H(l-s) \rangle \leq \frac{1}{\ln 2} 2^{r-s}, \quad (126)$$

where here the brackets denote the average. By choosing the compression level  $s$  sufficiently large, the exponent on the right hand side of Eq. (126) becomes sufficiently negative that the average Shannon information can be made arbitrarily small. Thus, given an upper bound on the Eavesdropper's Renyi information gain, the corrected data can be subjected to the reduction procedure of privacy amplification to yield an even shorter string on which the eavesdropper's Shannon information is arbitrarily low. The secrecy of the final key is recovered (but reduced in size) if an upper bound can be determined on the maximum Renyi information gain by the eavesdropper on corrected data.

The average secrecy capacity  $C'_s$  of a quantum cryptosystem is the number of secret bits produced per bit from the transmitter, and is given by

$$C'_s = \lim_{m \rightarrow \infty} \left\langle \frac{n - e_T - s}{m} \right\rangle. \quad (127)$$

Here the limit of a very long transmission is understood in which  $m$ , the number of bits of raw data, is very large.

The numerator of Eq. (127),  $(n - e_T - s)$ , is the size of the final key, where  $n$  is the number of bits of sifted data with the inconclusive bits removed,  $e_T$  is the number of bits of erroneous discarded data due to error correction, and  $s$  is the privacy amplification compression level. The average secrecy capacity, Eq. (127), converges in distribution to [19]

$$C'_s = \left\langle \frac{n}{m} \right\rangle \left( 1 - \left\langle \frac{e_T}{n} \right\rangle - \frac{t_F}{n} \Big|_{\frac{e_T}{n} = \langle \frac{e_T}{n} \rangle} - \lim_{m \rightarrow \infty} \left\langle \frac{q}{n} \right\rangle \right). \quad (128)$$

The factor  $\left\langle \frac{n}{m} \right\rangle$  in Eq. (128) is the conclusive rate. Since the inconclusive rate  $R_?$  is 1/2 for the BB84 protocol [11,19], and remains unchanged in the presence of the individual attack, the conclusive rate must also be 1/2, namely,

$$\left\langle \frac{n}{m} \right\rangle = (1 - R_?) = \left( 1 - \frac{1}{2} \right) = \frac{1}{2}. \quad (129)$$

Also in Eq. (128),  $\langle \frac{e_T}{n} \rangle$  is the average intrinsic error rate, and  $\langle \frac{g}{n} \rangle$  is the average information leakage during error correction. Since the present work focuses on the information leakage through eavesdropping (represented by the third term in Eq. (128)), possible additional terms,  $(-\langle \nu/n \rangle)$  and  $(-\langle g/n \rangle)$ , are dropped in Eq. (128) (See Eq. (123)). In the third term of Eq. (128),  $\frac{t_F}{n} |_{\frac{e_T}{n} = \langle \frac{e_T}{n} \rangle}$  is the average defense frontier  $t_F$  evaluated at the average intrinsic error rate. In the individual attack, each signal is attacked individually and in the same way, and it is assumed that the signal states, errors, and measurement outcomes of the probe and the legitimate receiver are all independently and identically distributed [19]. Multiple eavesdropping strategies are considered with different induced error rates, but the attack is restricted to the set of strategies yielding the greatest attainable expected Renyi information gain for a given expected error rate. The defense frontier  $t_F$  is, for all possible eavesdropping strategies, the upper bound on the information leakage through eavesdropping, based on an optimal eavesdropper in the limit of a long transmission. The defense frontier  $t_F$  is chosen to minimize the chance of any successful eavesdropping strategy, and, for the individual attack, it is given by [19]



$$t_F(n, e_T) = \max_{e \leq e_T} \left\{ n \left( 1 - \frac{e}{n} \right) I_{opt}^R \left( \frac{e}{n} + \xi \right) + \xi \left[ n^2 \left( 1 - \frac{e}{n} \right) \right]^{1/2} \right\}, \quad (130)$$

where  $I_{opt}^R(E)$  is the maximum Renyi information gain on corrected data by the eavesdropping probe, and conditional on fixed error rate  $E = (e/n)$ ; and  $\xi$  is defined by

$$\xi = \frac{1}{(2n)^{1/2}} \operatorname{erf}^{-1}(1 - p), \quad (131)$$

where  $\operatorname{erf}^{-1}$  denotes the inverse standard error function. The standard error function  $\operatorname{erf}(z)$  is defined by

$$\operatorname{erf}(z) = \frac{2}{\sqrt{\pi}} \int_0^z e^{-y^2} dy. \quad (132)$$

Also in Eq. (131),  $p$  is the probability for successful eavesdropping ( $I_R^T > t(n, e_T)$ ) on  $(n - e_T)$  bits of corrected data and producing  $e_T$  errors; and  $p$  can be made arbitrarily small. The defense frontier, Eq. (130), was determined by Slutsky, Rao, Sun, Tancevski, and Fainman [19] by clever use of the central limit theorem of probability theory, and is constructed to minimize the chance of successful eavesdropping. Using Eqs. (128)–(130), the asymptotic secrecy capacity, in the limit of long transmission with  $m \rightarrow \infty$ ,  $n \rightarrow \infty$ , and  $\xi \rightarrow 0$ , and for  $q = 0$ , becomes [19]

$$C'_s|_{q=0, n \rightarrow \infty, \xi \rightarrow 0} = \frac{1}{2} \left( 1 - E - \max_{E' \leq E} (1 - E') I_{opt}^R(E') \right), \quad (133)$$

where  $E$  is the error rate, and  $(\max_{x' \leq x} f(x'))$  denotes the maximum value of a function  $f(x')$  for  $x' \leq x$ . Also in Eq. (133),  $I_{opt}^R(E')$  is the maximum Renyi information gain on corrected data by the eavesdropping probe, conditional on fixed error rate  $E'$ . The asymptotic secrecy capacity, Eq. (133), is based on the definition of average secrecy capacity, Eq. (127), as given in the literature [19], however it is important to emphasize that the condition of maximum Renyi information gain by the eavesdropper may be overly conservative (See Section VI of Bennett, et al [9]).

Substituting Eq. (105) in Eq. (133), one obtains for the asymptotic secrecy capacity [13]:

$$C'_s|_{q=0, n \rightarrow \infty, \xi \rightarrow 0} = \begin{cases} \frac{1}{2} \left( 1 - E - \max_{E' \leq E} (1 - E') \log_2 \left[ 2 - \left( \frac{1 + (1 - 2 \csc^2 2\alpha) E'}{1 - E'} \right)^2 \right] \right), & \alpha \leq \pi/8 \\ \frac{1}{2} \left( 1 - E - \max_{E' \leq E} (1 - E') \log_2 \left[ 2 - \left( \frac{1 + (1 - 2 \sec^2 2\alpha) E'}{1 - E'} \right)^2 \right] \right), & \alpha \geq \pi/8 \end{cases}. \quad (134)$$

For  $\alpha = \pi/8$ , Eq. (134) also agrees with [19]. It is evident from Eqs. (104), (105), and (134) that as a function of  $\alpha$ , for fixed error rate, the overlap of

correlated probe states is greatest, the Renyi information gain by the probe is least, and the secrecy capacity is greatest for  $\alpha = \pi/8$ , which corresponds to the standard BB84 protocol [3] with  $\bar{\theta} = \pi/4$ .

## 8 SUMMARY

The maximum Renyi information gain, Eq. (105), by a Fuchs-Peres probe [11,15] is calculated for varying angle between the signal bases in the four-state protocol [3] of quantum key distribution. Two sets of optimized probe parameters, Eqs. (99) and (100) for  $\alpha \leq \pi/8$ , and Eqs. (101) and (102) for  $\alpha \geq \pi/8$ , are found to yield the optimization. Only a subset of one of these sets was found previously [11], for  $\alpha = \pi/8$  (Eq. (100) with  $\sin \lambda = 0$  and  $\alpha = \pi/8$ , or equivalently Eq. (90) with  $\sin \lambda = 0$ ). When the angle between the signal bases is the standard 45 degrees ( $\alpha = \pi/8$ ), the result of Slutsky, Rao, Sun, and Fainman [11] is recovered. Also, it was shown by explicit calculations that Eq. (105) gives the maximum information gain by the probe for a representative range of values of  $\alpha$ . Also, the maximum Renyi information, Eq. (105), for constant error rate, increases as  $\alpha$  decreases below  $\pi/8$ , or increases above  $\pi/8$ .

Also for  $\alpha = \pi/8$ , an additional set of optimum probe parameters, Eq. (119) previously ignored, has been found. A detailed comparison has been made between the optimizations of Ref. [12] and Ref. [11]. The reasons why the optimization of Ref. [11] (Eq. (106) above) did not yield the complete set of optimum probe parameters are because, in one approach considered there, the restriction in applicability of Eq. (28) was ignored. Also the parameter  $\mu$  was unnecessarily restricted in Eq. (106).

Next, following a review of the process of key distillation from the quantum transmission in quantum key distribution, the asymptotic secrecy capacity, Eq. (134), of the four-state protocol has been calculated for the case of an individual attack in which the eavesdropping probe is entangled with the signal states, and states of the probe become correlated with the states measured by the legitimate receiver. The calculation generalizes earlier work to include an arbitrary angle between the signal bases.

#### ACKNOWLEDGEMENTS

This work was supported by the U.S. Army Research Laboratory and the Defense Advanced Research Projects Agency. Useful communications with J. Myers, S. J. Lomonaco, J. D. Franson, J. D. Murley, and M. Foster are gratefully acknowledged. The author wishes to especially thank Prof. Young

S. Kim for inviting him to organize the sessions on quantum computing and quantum communication in which this paper was presented at the *First Feynman Festival*, 23–28 August, 2002 at the University of Maryland, College Park, MD.

## A Possible Extrema

In this appendix, the sets of conditions for the existence of possible extrema of the overlap of correlated probe states are determined by using Eqs. (69)–(71). Also, the possible extrema and the associated probe parameters are calculated. First, substituting Eq. (68) in Eq. (69), one obtains

$$\frac{\partial q}{\partial \lambda} + \frac{q - 1 + 2E}{[4(1 - E)^2 - c^2 \sin^2 2\alpha]} \sin^2 2\alpha c \frac{\partial c}{\partial \lambda} = 0. \quad (\text{A-1})$$

Using Eqs. (67) and (10), it follows that

$$\begin{aligned} \frac{\partial q}{\partial \lambda} = & -2 (\cos \lambda \sin \lambda) \{ (2 - \tan^2 2\alpha) [\cot^2 2\alpha - \cos 2\theta (\sin 2\phi + \cot^2 2\alpha)] \\ & + \sin 2\phi [1 + (1 - \tan^2 2\alpha) \cos 2\theta] \}, \end{aligned} \quad (\text{A-2})$$

$$c \frac{\partial c}{\partial \lambda} = -2 \cos^3 \lambda \sin \lambda \sin^2 2\theta \cos^2 2\phi. \quad (\text{A-3})$$

Then substituting Eqs. (A-2) and (A-3) in Eq. (A-1), one requires

$$\sin \lambda \cos \lambda F_1(\lambda, \theta, \phi) = 0, \quad (\text{A-4})$$

where

$$\begin{aligned} F_1(\lambda, \theta, \phi) = & 2 \{ (2 - \tan^2 2\alpha) [\cot^2 2\alpha - \cos 2\theta (\sin 2\phi + \cot^2 2\alpha)] \\ & + \sin 2\phi [1 + (1 - \tan^2 2\alpha) \cos 2\theta] \} \\ & + \frac{2(q-1+2E)}{4(1-E)^2 - c^2 \sin^2 2\alpha} \sin^2 2\alpha \cos^2 \lambda \sin^2 2\theta \cos^2 2\phi. \end{aligned} \quad (\text{A-5})$$

Next, substituting Eq. (68) in Eq. (70), one obtains

$$\frac{\partial q}{\partial \theta} + \frac{q - 1 + 2E}{[4(1 - E)^2 - c^2 \sin^2 2\alpha]} \sin^2 2\alpha c \frac{\partial c}{\partial \theta} = 0. \quad (\text{A-6})$$

Using Eqs. (67) and (10), it follows that

$$\frac{\partial q}{\partial \theta} = 2 \sin 2\theta \cos^2 \lambda \left( \sin 2\phi + 2 \cot^2 2\alpha - 1 \right), \quad (\text{A-7})$$

$$c \frac{\partial c}{\partial \theta} = 2 \sin 2\theta \cos^4 \lambda \cos 2\theta \cos^2 2\phi. \quad (\text{A-8})$$

Then substituting Eqs. (A-7) and (A-8) in Eq. (A-6), one requires

$$\sin 2\theta \cos^2 \lambda F_2(\lambda, \theta, \phi) = 0, \quad (\text{A-9})$$

where

$$\begin{aligned} F_2(\lambda, \theta, \phi) &= 2 (\sin 2\phi + 2 \cot^2 2\alpha - 1) \\ &+ \frac{2(q-1+2E)}{[4(1-E)^2 - c^2 \sin^2 2\alpha]} \sin^2 2\alpha \cos^2 \lambda \cos 2\theta \cos^2 2\phi. \end{aligned} \quad (\text{A-10})$$

Next, substituting Eq. (68) in Eq. (71), one obtains

$$\frac{\partial q}{\partial \phi} + \frac{q - 1 + 2E}{[4(1 - E)^2 - c^2 \sin^2 2\alpha]} \sin^2 2\alpha c \frac{\partial c}{\partial \phi} = 0. \quad (\text{A-11})$$

Using Eqs. (67) and (10), one gets

$$\frac{\partial q}{\partial \phi} = 2 \cos^2 \lambda \cos 2\phi (1 - \cos 2\theta), \quad (\text{A-12})$$

$$c \frac{\partial c}{\partial \phi} = -2 \cos^4 \lambda \sin^2 2\theta \sin 2\phi \cos 2\phi. \quad (\text{A-13})$$

Then substituting Eqs. (A-12) and (A-13) in Eq. (A-11), one requires

$$\cos^2 \lambda \cos 2\phi F_3(\lambda, \theta, \phi) = 0, \quad (\text{A-14})$$

where

$$F_3(\lambda, \theta, \phi) = 2(1 - \cos 2\theta) - \frac{2(q-1+2E)}{[4(1-E)^2 - c^2 \sin^2 2\alpha]} \sin^2 2\alpha \cos^2 \lambda \sin^2 2\theta \sin 2\phi. \quad (\text{A-15})$$

Summarizing Eqs. (A-4), (A-9), and (A-14), possible extrema of the overlap of correlated probe states are determined by

$$(a) \quad \sin \lambda \cos \lambda F_1(\lambda, \theta, \phi) = 0, \quad (\text{A-16})$$

$$(b) \quad \sin 2\theta \cos^2 \lambda F_2(\lambda, \theta, \phi) = 0, \quad (\text{A-17})$$

$$(c) \quad \cos^2 \lambda \cos 2\phi F_3(\lambda, \theta, \phi) = 0. \quad (\text{A-18})$$

Three possible ways of satisfying Eq. (A-16) are

$$(a1) \quad \sin \lambda = 0, \quad (\text{A-19})$$

$$(a2) \quad \cos \lambda = 0, \quad (\text{A-20})$$

$$(a3) \quad F_1 = 0. \quad (\text{A-21})$$



Two possible ways of satisfying Eq. (A-19) and (A-17) are

$$(a11) \quad \sin \lambda = 0, \quad \sin 2\theta = 0, \quad (A-22)$$

$$(a12) \quad \sin \lambda = 0, \quad F_2 = 0. \quad (A-23)$$

Two possible ways of satisfying Eqs. (A-22) and (A-18), and therefore also Eqs. (A-16) and (A-17), are

$$(a111) \quad \sin \lambda = 0, \quad \sin 2\theta = 0, \quad \cos 2\phi = 0, \quad (A-24)$$

$$(a112) \quad \sin \lambda = 0, \quad \sin 2\theta = 0, \quad F_3 = 0. \quad (A-25)$$

Two possible ways of satisfying Eqs. (A-23) and (A-18), and therefore also Eqs. (A-16) and (A-17), are

$$(a121) \quad \sin \lambda = 0, \quad \cos 2\phi = 0, \quad F_2 = 0, \quad (A-26)$$

$$(a122) \quad \sin \lambda = 0, \quad F_2 = 0, \quad F_3 = 0. \quad (A-27)$$

Equation (A-20) satisfies Eq. (A-17) and (A-18). Therefore, another way of satisfying Eqs. (A-16)–(A-18) is

$$(a2) \quad \cos \lambda = 0. \quad (A-28)$$

Three possible ways of satisfying Eqs. (A-21) and (A-17) are

$$(c1) \quad F_1 = 0, \quad \sin 2\theta = 0, \quad (A-29)$$

$$(c2) \quad F_1 = 0, \quad \cos \lambda = 0, \quad (A-30)$$

$$(c3) \quad F_1 = 0, \quad F_2 = 0. \quad (A-31)$$

Three possible ways of satisfying Eqs. (A-29) and (A-18), and therefore also Eqs. (A-16) and (A-17), are

$$(c11) \quad F_1 = 0, \quad \sin 2\theta = 0, \quad \cos 2\phi = 0, \quad (A-32)$$

$$(c12) \quad F_1 = 0, \quad \sin 2\theta = 0, \quad \cos \lambda = 0, \quad (A-33)$$

$$(c13) \quad F_1 = 0, \quad \sin 2\theta = 0, \quad F_3 = 0. \quad (A-34)$$

Eq. (A-30) satisfies Eq. (A-18), and therefore, another way of satisfying Eqs. (A-16)–(A-18) is

$$(c2) \quad F_1 = 0, \quad \cos \lambda = 0. \quad (A-35)$$

Three possible ways of satisfying Eqs. (A-31) and (A-18), and therefore also Eqs. (A-16) and (A-17), are

$$(c31) \quad F_1 = 0, \quad F_2 = 0, \quad \cos 2\phi = 0, \quad (A-36)$$

$$(c32) \quad F_1 = 0, \quad F_2 = 0, \quad \cos \lambda = 0, \quad (A-37)$$

$$(c33) \quad F_1 = 0, \quad F_2 = 0, \quad F_3 = 0. \quad (A-38)$$

Summarizing Eqs. (A-24)–(A-28) and (A-32)–(A-38), possible solutions to Eqs. (A-16)–(A-18) are determined by

$$(A) \quad \sin \lambda = 0, \quad \sin 2\theta = 0, \quad \cos 2\phi = 0, \quad (A-39)$$

$$(B) \quad \sin \lambda = 0, \quad \sin 2\theta = 0, \quad F_3 = 0, \quad (A-40)$$

$$(C) \quad \sin \lambda = 0, \quad \cos 2\phi = 0, \quad F_2 = 0, \quad (A-41)$$

$$(D) \quad \sin \lambda = 0, \quad F_2 = 0, \quad F_3 = 0, \quad (A-42)$$

$$(E) \quad \cos \lambda = 0, \quad (A-43)$$

$$(F) \quad \sin 2\theta = 0, \quad \cos 2\phi = 0, \quad F_1 = 0, \quad (A-44)$$

$$(G) \quad \cos \lambda = 0, \quad \sin 2\theta = 0, \quad F_1 = 0, \quad (A-45)$$

$$(H) \quad \sin 2\theta = 0, \quad F_1 = 0, \quad F_3 = 0, \quad (A-46)$$

$$(I) \quad \cos \lambda = 0, \quad F_1 = 0, \quad (A-47)$$

$$(J) \quad \cos 2\phi = 0, \quad F_1 = 0, \quad F_2 = 0, \quad (A-48)$$

$$(K) \quad \cos \lambda = 0, \quad F_1 = 0, \quad F_2 = 0, \quad (A-49)$$

$$(L) \quad F_1 = 0, \quad F_2 = 0, \quad F_3 = 0. \quad (A-50)$$

First consider possible extrema determined by possibility (B), Eq. (A-40):

$$\sin \lambda = 0, \quad (A-51)$$

$$\sin 2\theta = 0, \quad (\text{A-52})$$

$$F_3 = 0. \quad (\text{A-53})$$

From Eqs. (A-15), (A-52) and (A-53), it follows that

$$\cos 2\theta = 1. \quad (\text{A-54})$$

Substituting Eqs. (A-51) and (A-54) in Eq. (66), it follows that

$$\sin 2\phi = 1 - 2E \csc^2 2\alpha. \quad (\text{A-55})$$

Next substituting Eqs. (A-51), (A-52), and (A-54) in Eqs. (8)–(11), one obtains

$$a = \sin 2\phi, \quad (\text{A-56})$$

$$b = \sin 2\phi, \quad (\text{A-57})$$

$$c = 0, \quad (\text{A-58})$$

$$d = 1. \quad (\text{A-59})$$

Then substituting Eqs. (A-55)–(A-59) in Eq. (62), one obtains

$$Q = \frac{1 + (1 - 2 \csc^2 2\alpha) E}{1 - E}. \quad (\text{A-60})$$

For  $\alpha = \pi/8$ , Eq. (A-60) becomes Eq. (57), corresponding to the standard BB84 optimization [11], as must be the case.

Next, consider possibility (A), given by Eq. (A-39):

$$\sin \lambda = 0, \quad (\text{A-61})$$

$$\sin 2\theta = 0, \quad (\text{A-62})$$

$$\cos 2\phi = 0. \quad (\text{A-63})$$

From Eqs. (A-62) and (A-63), it follows that

$$\cos 2\theta = e_\theta, \quad (\text{A-64})$$

and

$$\sin 2\phi = e_\phi, . \quad (\text{A-65})$$

where

$$e_\theta = \pm 1, \quad e_\phi = \pm 1. \quad (\text{A-66})$$

Substituting Eqs. (A-61), (A-64), and (A-65) in Eq. (65), then one requires

$$E = \frac{1}{2} \left[ 1 - e_\theta + e_\theta (1 - e_\phi) \sin^2 2\alpha \right]. \quad (\text{A-67})$$

Next substituting Eqs. (A-61)–(A-66) in Eqs. (8)–(11), one obtains

$$a = e_\theta e_\phi, \quad (\text{A-68})$$

$$b = e_\phi, \quad (\text{A-69})$$

$$c = 0, \quad (\text{A-70})$$

$$d = e_\theta. \quad (\text{A-71})$$

Then substituting Eqs. (A-67)–(A-71) in Eq. (62), one obtains

$$Q = \frac{e_\phi (1 + e_\theta) + e_\theta (1 - e_\phi) \sin^2 2\alpha}{(1 + e_\theta) - e_\theta (1 - e_\phi) \sin^2 2\alpha}. \quad (\text{A-72})$$

For  $e_\theta = \pm 1$  and  $e_\phi = +1$ , Eq. (A-72) yields

$$Q = 1. \quad (\text{A-73})$$

For  $e_\theta = \pm 1$  and  $e_\phi = -1$ , Eq. (A-72) yields

$$Q = -1. \quad (\text{A-74})$$

One concludes that possibility (A), Eq. (A-39), does not yield the minimum overlap.

Next, consider possibility (C), given by Eq. (A-41):

$$\sin \lambda = 0, \quad (\text{A-75})$$

$$\cos 2\phi = 0, \quad (\text{A-76})$$

$$F_2 = 0. \quad (\text{A-77})$$

Next, substituting Eqs. (A-10) and (A-76) in Eq. (A-77), one obtains

$$\sin 2\phi = 1 - 2 \cot^2 2\alpha. \quad (\text{A-78})$$

Then combining Eqs. (A-76) and (A-78), one requires:

$$\cot^2 2\alpha = \frac{1}{2} (1 - e_\phi), \quad (\text{A-79})$$

and therefore, using Eq. (A-66), one requires  $e_\phi = -1$ , and

$$\alpha = \pi/8. \quad (\text{A-80})$$

Furthermore, using Eqs. (A-75), (A-76), and (A-80) in Eq. (66), one requires:

$$E = \frac{1}{2}. \quad (\text{A-81})$$

Therefore possibility (C) does not yield a solution.

Next consider possibility (D), given by Eq. (A-42):

$$\sin \lambda = 0, \quad (\text{A-82})$$

$$F_2 = 0, \quad (\text{A-83})$$

$$F_3 = 0. \quad (\text{A-84})$$

Using Eqs. (A-82) and (10), one has

$$c = \sin 2\theta \cos 2\phi. \quad (\text{A-85})$$

Also, using Eqs. (A-83) and (A-10), one requires

$$\left[ \frac{q - 1 + 2E}{4(1 - E)^2 - c^2 \sin^2 2\alpha} \right] = \frac{1 - 2 \cot^2 2\alpha - \sin 2\phi}{\sin^2 2\alpha \cos 2\theta \cos^2 2\phi}. \quad (\text{A-86})$$

Also, Eqs. (A-84) and (A-15) require

$$\left[ \frac{q - 1 + 2E}{4(1 - E)^2 - c^2 \sin^2 2\alpha} \right] = \frac{1 - \cos 2\theta}{\sin^2 2\alpha \sin^2 2\theta \sin 2\phi}. \quad (\text{A-87})$$

Furthermore using Eq. (A-82), Eq. (67) becomes

$$\begin{aligned} q = & (2 - \tan^2 2\alpha) [\cot^2 2\alpha - \cos 2\theta (\sin 2\phi + \cot^2 2\alpha)] \\ & + \sin 2\phi [1 + (1 - \tan^2 2\alpha) \cos 2\theta] - 4E \csc^2 2\alpha + 3. \end{aligned} \quad (\text{A-88})$$

Next equating Eqs. (A-86) and (A-87) requires

$$\begin{aligned} (1 - 2 \cot^2 2\alpha - \sin 2\phi) \sin^2 2\theta \sin 2\phi \\ = (1 - \cos 2\theta) \cos 2\theta \cos^2 2\phi. \end{aligned} \quad (\text{A-89})$$

Next, multiplying Eq. (66) by  $\sin^2 \lambda$  and substituting Eq. (A-82), one gets

$$\cos 2\theta = \frac{1 - 2E}{1 - \sin^2 2\alpha (1 - \sin 2\phi)}. \quad (\text{A-90})$$

Then substituting Eq. (A-90) in Eq. (A-89), one obtains

$$\begin{aligned} & (1 - 2 \cot^2 2\alpha - \sin 2\phi) \sin 2\phi \\ & \times \left\{ \left[ 1 - \sin^2 2\alpha (1 - \sin 2\phi) \right]^2 - (1 - 2E)^2 \right\} \\ & = (1 - 2E) \cos^2 2\phi \left[ 1 - \sin^2 2\alpha (1 - \sin 2\phi) - (1 - 2E) \right], \end{aligned} \quad (\text{A-91})$$



or equivalently,

$$\begin{aligned} & \left[ 1 - \sin^2 2\alpha (1 - \sin 2\phi) - (1 - 2E) \right] \{ (1 - 2E) \cos^2 2\phi \\ & - (1 - 2 \cot^2 2\alpha - \sin 2\phi) \sin 2\phi \left[ 1 - \sin^2 2\alpha (1 - \sin 2\phi) + (1 - 2E) \right] \} = 0. \end{aligned} \quad (\text{A-92})$$

Therefore, either

$$\left[ 1 - \sin^2 2\alpha (1 - \sin 2\phi) - (1 - 2E) \right] = 0, \quad (\text{A-93})$$

or else,

$$\begin{aligned} & (1 - 2E) \cos^2 2\phi - (1 - 2 \cot^2 2\alpha - \sin 2\phi) \sin 2\phi \\ & \times \left[ 1 - \sin^2 2\alpha (1 - \sin 2\phi) + (1 - 2E) \right] = 0. \end{aligned} \quad (\text{A-94})$$

Equation (A-93) gives

$$\sin 2\phi = 1 - 2E \csc^2 2\alpha, \quad (\text{A-95})$$

which when substituted in Eq. (A-90) gives

$$\cos 2\theta = 1, \quad (\text{A-96})$$

and substituting Eqs. (A-82), (A-95), (A-96) and (8)–(11) in Eq. (62), one again obtains the same solution resulting from possibility (B), Eqs. (A-55)–(A-60). However Eq. (A-95) must also be compatible with the remaining requirements if possibility (D) is to represent a solution.

Alternatively, one has Eq. (A-94), which becomes the cubic:

$$a_1 \sin^3 2\phi + a_2 \sin^2 2\phi + a_3 \sin 2\phi + a_4 = 0, \quad (\text{A-97})$$

where

$$a_1 = \sin^2 2\alpha, \quad (\text{A-98})$$

$$a_2 = 3 - 4 \sin^2 2\alpha, \quad (\text{A-99})$$

$$a_3 = (2E - \cos^2 2\alpha - 1) (1 - 2 \cot^2 2\alpha), \quad (\text{A-100})$$

$$a_4 = (1 - 2E). \quad (\text{A-101})$$

The possible solutions to the cubic Eq. (A-97) are given by

$$\sin 2\phi = x - \frac{p}{3}, \quad (\text{A-102})$$

$$\sin 2\phi = x_+ - \frac{p}{3}, \quad (\text{A-103})$$

$$\sin 2\phi = x_- - \frac{p}{3}, \quad (\text{A-104})$$

where

$$x = c_+ + c_-, \quad (\text{A-105})$$

$$x_{\pm} = -\frac{1}{2} (c_+ + c_-) \pm \frac{3^{1/2}}{2} i (c_+ - c_-), \quad (\text{A-106})$$

$$c_{\pm} = \left[ -\frac{B}{2} \pm \left( \frac{B^2}{4} + \frac{A^3}{27} \right)^{1/2} \right]^{1/3}, \quad (\text{A-107})$$

$$A = \frac{1}{3} (3q - p^2), \quad (\text{A-108})$$

$$B = \frac{1}{27} (2p^3 - 9pq + 27r), \quad (\text{A-109})$$

$$p = \frac{a_2}{a_1}, \quad (\text{A-110})$$

$$q = \frac{a_3}{a_1}, \quad (\text{A-111})$$

$$r = \frac{a_4}{a_1}. \quad (\text{A-112})$$

Next, substituting Eqs. (A-85) and (A-90) in Eq. (A-87), one obtains

$$\begin{aligned} & \left[ 2E - \sin^2 2\alpha (1 - \sin 2\phi) \right] \left[ 4(1 - E)^2 - \frac{[2(1 - E) - \sin^2 2\alpha (1 - \sin 2\phi)]}{[1 - \sin^2 2\alpha (1 - \sin 2\phi)]^2} \right] \\ & \times \left\{ \left[ 2E - \sin^2 2\alpha (1 - \sin 2\phi) \right] \sin^2 2\alpha \cos^2 2\phi + \left[ 1 - \sin^2 2\alpha (1 - \sin 2\phi) \right] \right. \\ & \quad \left. \times (q - 1 + 2E) \sin^2 2\alpha \sin 2\phi \right\} = 0. \end{aligned} \quad (\text{A-113})$$

Therefore, either

$$\left[ 2E - \sin^2 2\alpha (1 - \sin 2\phi) \right] = 0, \quad (\text{A-114})$$

or else,

$$\begin{aligned} & 4(1 - E)^2 = \frac{[2(1 - E) - \sin^2 2\alpha (1 - \sin 2\phi)]}{[1 - \sin^2 2\alpha (1 - \sin 2\phi)]^2} \\ & \times \left\{ \left[ 2E - \sin^2 2\alpha (1 - \sin 2\phi) \right] \sin^2 2\alpha \cos^2 2\phi + \left[ 1 - \sin^2 2\alpha (1 - \sin 2\phi) \right] \right. \\ & \quad \left. \times (q - 1 + 2E) \sin^2 2\alpha \sin 2\phi \right\}. \end{aligned} \quad (\text{A-115})$$

Equation (A-114) gives

$$\sin 2\phi = 1 - 2E \csc^2 2\alpha, \quad (\text{A-116})$$

which together with Eqs. (A-90), (A-82), (8)–(11), and (62) again yields the same result as possibility (B), Eqs. (A-55)–(A-60). However, Eqs. (A-95) and (A-116) must also be compatible with the remaining restrictions, if possibility (D) is to represent a solution.

Alternatively, one has Eq. (A-115). The quantity  $q$  appearing in Eq. (A-115) and given by Eq. (A-88) reduces using Eq. (A-90) to

$$q = \sin 2\phi + \frac{(1 + \sin 2\phi)(1 - 2E)}{\cos^2 2\alpha + \sin^2 2\alpha \sin 2\phi}. \quad (\text{A-117})$$

Then substituting Eq. (A-117) in Eq. (A-115), one obtains the cubic:

$$b_1 \Lambda^3 + b_2 \Lambda^2 + b_3 \Lambda + b_4 = 0, \quad (\text{A-118})$$

where

$$\Lambda = \cos^2 2\alpha + \sin^2 2\alpha \sin 2\phi, \quad (\text{A-119})$$

$$b_1 = (1 - 2E) (1 - 2 \csc^2 2\alpha), \quad (\text{A-120})$$

$$b_2 = 4(1 - E)^2 - \sin^2 2\alpha + (1 - 2E)^2 (1 - 2 \csc^2 2\alpha) \quad (\text{A-121})$$

$$-(1 - 2E) (1 + \cos^2 2\alpha - 4 \cot^2 2\alpha),$$

$$b_3 = -(1 - 2E)^2 (1 + \cos^2 2\alpha - 4 \cot^2 2\alpha) + (1 - 2E) \cos^2 2\alpha (1 - 2 \cot^2 2\alpha), \quad (\text{A-122})$$

$$b_4 = (1 - 2E)^2 (1 - 2 \cos^2 2\alpha \cot^2 2\alpha). \quad (\text{A-123})$$

(In obtaining Eq. (A-118), an overall factor of  $\Lambda$  was removed and ignored, since  $\Lambda = 0$  can only be satisfied if  $E = 1/2$ .)

Next, substituting Eqs. (A-85), (A-90) and (A-117) in Eq. (A-86), leads to the quintic:

$$c_1 \sin^5 2\phi + c_2 \sin^4 2\phi + c_3 \sin^3 2\phi + c_4 \sin^2 2\phi + c_5 \sin 2\phi + c_6 = 0, \quad (\text{A-124})$$

where

$$c_1 = \sin^6 2\alpha, \quad (\text{A-125})$$

$$c_2 = \sin^4 2\alpha (5 \cos^2 2\alpha + 2E - 2), \quad (\text{A-126})$$

$$\begin{aligned} c_3 = & \sin^4 2\alpha (5 - 12E + 8E^2) - \sin^2 2\alpha \cos^2 2\alpha (1 - 2E) - 2 \sin^2 2\alpha (1 - 2E)^2 \\ & - 2 \sin^4 2\alpha \cos^2 2\alpha + 5 \sin^2 2\alpha \cos^4 2\alpha - \sin^6 2\alpha, \end{aligned} \quad (\text{A-127})$$

$$\begin{aligned} c_4 = & (1 - 2 \cot^2 2\alpha) [\sin^2 2\alpha (1 - 2E)^2 - 4 \sin^4 2\alpha (1 - E)^2 + \sin^6 2\alpha \\ & - \sin^2 2\alpha \cos^4 2\alpha] - 2 \sin^4 2\alpha \cos^2 2\alpha - \sin^4 2\alpha (1 - 2E)^2 \\ & + \sin^4 2\alpha (1 - 2E) + 8 \sin^2 2\alpha \cos^2 2\alpha (1 - E)^2, \end{aligned} \quad (\text{A-128})$$

$$\begin{aligned}
c_5 = (1 - 2 \cot^2 2\alpha) & \left[ -8 \sin^2 2\alpha \cos^2 2\alpha (1 - E)^2 + 2 \sin^4 2\alpha \cos^2 2\alpha \right] \\
& + 4 \cos^4 2\alpha (1 - E)^2 + \sin^2 2\alpha (2 - \sin^2 2\alpha) (1 - 2E)^2 \\
& + \sin^2 2\alpha \cos^2 2\alpha (1 - 2E) - \sin^2 2\alpha \cos^4 2\alpha,
\end{aligned} \tag{A-129}$$

$$\begin{aligned}
c_6 = (1 - 2 \cot^2 2\alpha) & \left[ \sin^2 2\alpha \cos^4 2\alpha - 4 \cos^4 2\alpha (1 - E)^2 - \sin^2 2\alpha (1 - 2E)^2 \right] \\
& + \sin^4 2\alpha (1 - 2E)^2.
\end{aligned} \tag{A-130}$$

In summary, the possibility (D) requires that one of the following three sets of equations be satisfied:

$$(i) \text{ Eqs. (A-97), (A-118), and (A-124);} \tag{A-131}$$

$$(ii) \text{ Eqs. (A-95), (A-118), and (A-124);} \tag{A-132}$$

$$(iii) \text{ Eqs. (A-95) and (A-124).} \tag{A-133}$$

But none of these alternatives, (i), (ii), or (iii) can be satisfied. It can be shown numerically that Eqs. (A-97), (A-118), and (A-124) cannot be simultaneously satisfied. Evidently, it can also be shown numerically that Eqs. (A-95) and (A-124) cannot be simultaneously satisfied. (This has been verified explicitly for  $\alpha = \pi/9$ ,  $\pi/8$ , and  $\pi/5$ .) Thus, possibility (D) apparently does not produce a solution.

Next, consider possibility (E), given by Eq. (A-43):

$$\cos \lambda = 0. \quad (\text{A-134})$$

Substituting Eq. (A-134) in Eq. (66), one has

$$\sin 2\mu = 1 - 2E \csc^2 2\alpha. \quad (\text{A-135})$$

Next substituting Eqs. (A-134) and (A-135) in Eqs. (8)–(11), one obtains

$$a = 1 - 2E \csc^2 2\alpha, \quad (\text{A-136})$$

$$b = 1 - 2E \csc^2 2\alpha, \quad (\text{A-137})$$

$$c = 0, \quad (\text{A-138})$$

$$d = 1. \quad (\text{A-139})$$

Then substituting Eqs. (A-136)–(A-139) in Eq. (62), one again obtains Eq. (A-60). Therefore, possibility (E), Eq. (A-43), gives the same result as possibility (B), Eq. (A-40). Note however that the probe parameter  $\mu$  is restricted by Eq. (A-135), and the probe parameter  $\phi$  is unrestricted, while for possibility (B),  $\phi$  is restricted by Eq. (A-55), and  $\mu$  is unrestricted. This is addressed in Section 4.

Next, consider possibility (F), given by Eq. (A-44):

$$\sin 2\theta = 0, \quad (\text{A-140})$$

$$\cos 2\theta = e_\theta, \quad (\text{A-141})$$

$$\cos 2\phi = 0, \quad (\text{A-142})$$

$$\sin 2\phi = e_\phi, \quad (\text{A-143})$$

$$F_1 = 0. \quad (\text{A-144})$$

Substituting Eqs. (A-5), and (A-140)–(A-143) in Eq. (A-144), one requires

$$(1 - e_\theta) \left[ e_\phi \cot^2 2\alpha \left( 2 - \tan^2 2\alpha \right) + 1 \right] = 0, \quad (\text{A-145})$$

and therefore

$$e_\theta = 1. \quad (\text{A-146})$$

Next substituting Eqs. (A-141), (A-146), and (A-143) in Eq. (66), one gets

$$\sin 2\mu = \frac{\sin^2 2\alpha (1 - e_\phi \cos^2 \lambda) - 2E}{\sin^2 2\alpha \sin^2 \lambda}. \quad (\text{A-147})$$

Then substituting Eqs. (A-140)–(A-143), (A-146) and (A-147) in Eqs. (8)–(11), one again obtains Eqs. (A-136)–(A-139), and (A-60). Thus possibility (F), Eq. (A-44), also gives the same result as possibility (B), Eq. (A-40). Note



however that the probe parameters  $\mu$  and  $\lambda$  are restricted by Eq. (A-147).

This is addressed in Section 4.

Next consider possibility (G), given by Eq. (A-45):

$$\cos \lambda = 0, \quad (\text{A-148})$$

$$\sin 2\theta = 0 \quad (\text{A-149})$$

$$\cos 2\theta = e_\theta, \quad (\text{A-150})$$

$$F_1 = 0. \quad (\text{A-151})$$

Substituting Eq. (A-148) in Eq. (66), one gets

$$\sin 2\mu = 1 - 2E \csc^2 2\alpha. \quad (\text{A-152})$$

Substituting Eqs. (A-5) and (A-148)–(A-150) in Eq. (A-151), one obtains

$$(1 - e_\theta) \left[ \sin 2\phi + \cot^2 2\alpha (2 - \tan^2 2\alpha) \right] = 0. \quad (\text{A-153})$$

Therefore, one requires

$$e_\theta = 1, \quad (\text{A-154})$$

or alternatively,

$$\sin 2\phi = 1 - 2 \cot^2 2\alpha. \quad (\text{A-155})$$

Substituting Eqs. (A-148), (A-149), and (A-152) in Eqs. (8)–(11), one again obtains Eqs. (A-136)–(A-139) and (A-60). The differing values of the probe parameters are addressed in Section 4.

Next consider possibility (H), given by Eq. (A-46):

$$\sin 2\theta = 0 \tag{A-156}$$

$$\cos 2\theta = e_\theta, \tag{A-157}$$

$$F_1 = 0, \tag{A-158}$$

$$F_3 = 0. \tag{A-159}$$

Substituting Eqs. (A-15) and (A-156) in Eq. (A-159), one gets

$$\cos 2\theta = 1, \tag{A-160}$$

and therefore

$$e_\theta = 1 \tag{A-161}$$

in Eq. (A-157). Next using Eqs. (A-5) and (A-160), one sees that Eq. (A-158) is satisfied. Also, substituting Eq. (A-160) in Eq. (66), one obtains

$$\sin 2\mu = \frac{\sin^2 2\alpha (1 - \cos^2 \lambda \sin 2\phi) - 2E}{\sin^2 2\alpha \sin^2 \lambda}. \tag{A-162}$$

Then substituting Eqs. (A-156), (A-160), and (A-162) in Eqs. (8)–(11), one again obtains Eqs. (A-136)–(A-139) and (A-60). The differing values of the probe parameters are addressed in Section 4.

Next consider possibility (I), given by Eq. (A-47):

$$\cos \lambda = 0 \tag{A-163}$$

$$F_1 = 0, \tag{A-164}$$

Substituting Eqs. (A-163) in Eq. (66), one gets

$$\sin 2\mu = 1 - 2E \csc^2 2\alpha. \tag{A-165}$$

Next substituting Eqs. (A-5) and (A-163) in Eq. (A-164), one obtains

$$(1 - \cos 2\theta) \left[ \sin 2\phi + 2 \cot^2 2\alpha - 1 \right] = 0. \tag{A-166}$$

Therefore one requires

$$\cos 2\theta = 1, \tag{A-167}$$

or else,

$$\sin 2\phi = 1 - 2 \cot^2 2\alpha. \tag{A-168}$$

Using Eqs. (A-163), (A-165), and (A-167) or (A-168) in Eqs. (8)–(11), one again obtains Eqs. (A-136)–(A-139) and (A-60). The differing values of the probe parameters are addressed in Section 4.

Next consider possibility (J), given by Eqs. (A-48):

$$\cos 2\phi = 0, \tag{A-169}$$

$$\sin 2\phi = e_\phi, \tag{A-170}$$

$$F_1 = 0, \tag{A-171}$$

$$F_2 = 0. \tag{A-172}$$

Then substituting Eqs. (A-10) and (A-170) in Eq. (A-172), one gets

$$\cot^2 2\alpha = \frac{1}{2} (1 - e_\phi), \tag{A-173}$$

which cannot be satisfied for arbitrary  $\alpha$ . Therefore possibility (J) cannot represent a solution for arbitrary  $\alpha$ . (It is to be noted however that Eq. (A-173) is satisfied if  $e_\rho = -1$ , and  $\alpha = \pi/8$ . This particular case is addressed in Section 6, following Eq. (119).)

Next consider possibility (K), given by Eqs. (A-49):

$$\cos \lambda = 0, \tag{A-174}$$

$$F_1 = 0, \tag{A-175}$$

$$F_2 = 0. \tag{A-176}$$

Substituting Eqs. (A-10) and (A-174) in Eq. (A-176), one obtains

$$\sin 2\phi = 1 - 2 \cot^2 2\alpha. \quad (\text{A-177})$$

Next substituting Eqs. (A-5), (A-174), and (A-177) in Eq. (A-175), one gets the trivial identity:

$$\begin{aligned} (2 - \tan^2 2\alpha) [\cot^2 2\alpha - \cos 2\theta (1 - \cot^2 2\alpha)] \\ + (1 - 2 \cot^2 2\alpha) [1 + (1 - \tan^2 2\alpha) \cos 2\theta] = 0 \end{aligned} \quad (\text{A-178})$$

for any  $\cos 2\theta$ . Then substituting Eq. (A-174) in Eq. (66), one obtains

$$\sin 2\mu = 1 - 2E \csc^2 2\alpha, \quad (\text{A-179})$$

and, using Eqs. (A-174), (A-179), (8)–(11), and (62), then Eqs. (A-136)–(A-139) and (A-60) again follow. The differing values of the probe parameters are addressed in Section 4.

Next consider possibility (L), given by Eqs. (A-50):

$$F_1 = 0, \quad (\text{A-180})$$

$$F_2 = 0, \quad (\text{A-181})$$

$$F_3 = 0. \quad (\text{A-182})$$

From Eqs. (A-5) and (A-180), it follows that

$$\begin{aligned} & \sin^2 2\alpha \cos^2 \lambda \left[ \frac{2(q-1+2E)}{4(1-E)^2 - c^2 \sin^2 2\alpha} \right] \\ &= \frac{-2\{(2-\tan^2 2\alpha)[\cot^2 2\alpha - \cos 2\theta(\sin 2\phi + \cot^2 2\alpha)] + \sin 2\phi[1 + (1-\tan^2 2\alpha)\cos 2\theta]\}}{\sin^2 2\theta \cos^2 2\phi}. \end{aligned} \quad (\text{A-183})$$

From Eqs. (A-10) and (A-181), one gets

$$\sin^2 2\alpha \cos^2 \lambda \left[ \frac{2(q-1+2E)}{4(1-E)^2 - c^2 \sin^2 2\alpha} \right] = \frac{-2(\sin 2\phi + 2\cot^2 2\alpha - 1)}{\cos 2\theta \cos^2 2\phi}. \quad (\text{A-184})$$

From Eqs. (A-15) and (A-182), one gets

$$\sin^2 2\alpha \cos^2 \lambda \left[ \frac{2(q-1+2E)}{4(1-E)^2 - c^2 \sin^2 2\alpha} \right] = \frac{2(1 - \cos 2\theta)}{\sin^2 2\theta \sin 2\phi}. \quad (\text{A-185})$$

Next equating Eqs. (A-183) and (A-185) leads to

$$\cos 2\theta = 1, \quad (\text{A-186})$$

and Eqs. (A-183) and (A-185) are both identically satisfied. But then substituting Eq. (A-186), (67), and (10) in Eq. (A-184), one obtains

$$\sin^2 2\alpha \cos^2 \lambda \cos^2 2\phi \left[ 1 + (1 - 2\csc^2 2\alpha) E \right] = -2(1 - E)^2 (\sin 2\phi + 2\cot^2 2\alpha - 1), \quad (\text{A-187})$$

or

$$\cos^2 \lambda = \frac{2(1 - E)^2 (1 - 2\cot^2 2\alpha - \sin 2\phi)}{\sin^2 2\alpha \cos^2 2\phi [1 + (1 - 2\csc^2 2\alpha) E]}. \quad (\text{A-188})$$

Also, substituting Eq. (A-186) in Eq. (66), one obtains

$$\sin 2\mu \sin^2 \lambda = 1 - 2E \csc^2 2\alpha - \cos^2 \lambda \sin 2\phi. \quad (\text{A-189})$$

Then substituting Eqs. (A-188) and (A-189) in Eqs. (8)–(11) yields

$$a = 1 - 2E \csc^2 2\alpha, \quad (\text{A-190})$$

$$b = 1 - 2E \csc^2 2\alpha, \quad (\text{A-191})$$

$$c = 0, \quad (\text{A-192})$$

$$d = 1. \quad (\text{A-193})$$

Next substituting Eqs. (A-190)–(A-193) in Eq. (62) again leads to

$$Q = \frac{1 + (1 - 2 \csc^2 2\alpha) E}{1 - E}. \quad (\text{A-194})$$

The differing values of the probe parameters are addressed in Section 4.

## REFERENCES

- [1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, “Quantum cryptography,” *Rev. Mod. Phys.* **74**, 145–195 (2002).
- [2] S. Wiesner, “Conjugate coding,” *SIGACT News* **15**, 78–88 (1983).
- [3] C. H. Bennett and G. Brassard, “Quantum cryptography: public key distribution and coin tossing,” in *Proceedings of the IEEE International Con-*

ference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp. 175–179.

[4] C. H. Bennett and G. Brassard, “Quantum public key distribution system,” IBM Tech. Discl. Bull. **28**, 3153–3163 (1985).

[5] G. Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communication, ” J. Am. Inst. Electr. Eng. **45**, 295–301 (1926).

[6] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” Phys. Rev. Lett. **68**, 3121–3124 (1992).

[7] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” Phys. Rev. Lett. **67**, 661–663 (1991).

[8] H. E. Brandt, “Positive operator valued measure in quantum information processing,” Am. J. Phys. **67**, 434–439 (1999).

[9] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, “Generalized privacy amplification,” IEEE Trans. Inf. Theor. **41**, 1915–1923 (1995).

[10] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, “Experimental quantum cryptography,” J. Cryptology **5**, 3–28 (1992).

[11] B. A. Slutsky, R. Rao, P. C. Sun, and Y. Fainman, “Security of



quantum cryptography against individual attacks,” *Phys. Rev. A* **57**, 2383–2398 (1998).

[12] H. E. Brandt, “Probe Optimization in four-state protocol of quantum cryptography,” *Phys. Rev. A* **66**, 032303-1-16 (2002).

[13] H. E. Brandt, “Secrecy capacity in the four-state protocol of quantum key distribution,” *J. Math. Phys.* **43**, 4526-4530 (2002).

[14] H. E. Brandt, “Optimization Problem in Quantum Cryptography,” to appear in *J. Opt. B* (2003).

[15] C. A. Fuchs and A. Peres, “Quantum-state disturbance versus information gain: uncertainty relations for quantum information,” *Phys. Rev. A* **53**, 2038–2045 (1996).

[16] H. E. Brandt, “Eavesdropping optimization for quantum cryptography using a positive operator valued measure,” *Phys. Rev. A* **59**, 2665–2669 (1999).

[17] H. E. Brandt, “Inconclusive rate as a disturbance measure in quantum cryptography,” *Phys. Rev. A* **62**, 042310-1-14 (2000).

[18] H. E. Brandt, “Inconclusive rate in quantum key distribution,” *Phys. Rev. A* **64**, 042316-1-5 (2001).

[19] B. Slutsky, R. Rao, P. C. Sun, L. Tancevski, and S. Fainman, “Defense

frontier analysis of quantum cryptographic systems,” *Applied Optics* **37**,  
2869–2878 (1998).